U.S. General Services Administration (GSA)

PRESIDENTIAL TRANSITION "HOT ISSUES" INFORMATION PAPER

SUBJECT: Enabling Cloud in Government

BACKGROUND:

TTS administers two distinct programs that enable secure cloud use among government agencies, **FedRAMP** and **cloud.gov.**

FedRAMP

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments.

FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

a. Issues:

- Reducing the Time to Achieve a FedRAMP Authorization: In years past, the time to obtain a FedRAMP Authorization was between 12-18 months. The length of this process did not include upfront time spent by cloud service offerings (CSOs) to achieve necessary compliance with federal policies and standards. In order to make necessary improvements to the program that would reduce the time for authorizations and to incent more CSOs to enter the Federal marketplace, FedRAMP has kicked off a major transformation effort, called FedRAMP Accelerated, within the last year to steamline its processes with the goal of becoming more efficient and agile, without sacrificing the crucial, rigorous cybersecurity reviews. This process included more than 80 interviews with agencies, industry, the Joint Authorization Board (which consists of the Chief Information Officers for GSA, DoD, and DHS), and Third Party Assessment Organizations (3PAOs) to develop experience maps and truly understand the process and pain points for these key stakeholder groups. Preliminary results from the pilot are showing the time to Authorization has been significantly reduced, by approximately 4 months.
- Streamlined Authorization Approach for Low Impact Software Solutions: In previous years, FedRAMP has focused on enterprise-wide solutions with the establishment of the current security requirements. This is a "one size fits all" model that does not work well for simple software solutions in the cloud. Services like Trello, Doodle, or SurveyMonkey, among numerous other examples, are used for niche reasons and only contain certain data types. FedRAMP is developing a streamlined approach for niche providers by working with 18F,

GSA's Chief Technology Officer, and digital service teams across the government.

- Reducing Effort For Continued Authorizations: After an authorization is granted, cloud providers and the government must ensure systems remain secure — similar to standard technology operations and maintenance(O&M) costs and activities. FedRAMP ensures these activitiesare completed through "continuous monitoring," which involves monthly and yearly reporting, analysis of changes to systems, and responding to any breaches or incidents. The level of effort for continuous monitoring is significant, and FedRAMP will be working with the DHS Continuous Diagnostics and Mitigation (CDM) program to make the process as efficient and automated as possible, in order to reduce the level of effort for the government and industry.

1. **SCOPE AND EFFECT:**
   a. Impact on GSA's Customers:
      - A FedRAMP Authorization is required prior to an Agency using a CSO, which impacts the speed at which cloud technologies are adopted across the government.
      - Having a faster time to authorization, while still ensuring appropriate security processes and protocols are in place, is critical to ensure that agencies are able to use the latest and greatest IT solutions.
      - Reducing the burden for continued authorizations will allow the government to use more services by ensuring O&M costs do nott overly burden IT shops.
   b. Impact on the Private Sector and State & Local Governments:
      - The private sector must comply with the FedRAMP requirements and ensure appropriate security for Federal data. A FedRAMP Authorization is required to gain and maintain government customers and process Federal data. This impacts the private sector's time to offer their CSO to the federal marketplace.
      - Cost for authorizations has steadily increased due to the increased visibility of cyber attacks, and any effort to streamline and automate the process will lower the barrier to entry for private industry.

2. **ACTION(S) PLANNED OR REQUIRED:**

- Reducing the Time to Achieve a FedRAMP Authorization: In the next 6 months, FedRAMP will release the final FedRAMP Accelerated authorization process which condenses the authorization timeline from 12-18 months to 3-6 months. FedRAMP Accelerated also includes a rapid route to a "FedRAMP Ready" designation which can be achieved in 4-8 weeks, involving an on-site validation of CSO capabilities that is intended to act as an indicator of a CSO's ability to achieve a full FedRAMP Authorization.
- Streamlined Authorization Approach for Low Impact Software Solutions: FedRAMP has partnered with GSA CIO, CTO, 18F, and OMB to develop a risk-based framework that can be applied to specific Agency data-types and use cases. This framework will be presented to the CIO Council for review and agreement in Calendar Year 2016 and will

be publicly vetted at the beginning of the new year and incorporate private industry feedback. The goal is to have the new process finalized by Q2 or Q3 in FY17.

- Reducing Effort For Continued Authorizations: During FY17, in partnership with the DHS CDM office, FedRAMP will complete a redesign effort for continuous monitoring. This will include a full scale outreach campaign with stakeholders (including customer journey mapping) and redesign efforts with NIST and others. This effort is expected to take 6-9 months to complete and is projected to conclude by the end of FY17.

3. KEY STAKEHOLDER INTEREST:

FedRAMP is a highly visible program with a complex, intertwined set of stakeholders including:

- OMB — acts primarily as oversight but is also a FedRAMP Authorized CSO with two service offerings;
- Joint Authorization Board (JAB) — includes DHS, DOD, and GSA CIOs providing overall governance and support to FedRAMP. These offices receive direct funding for FedRAMP in addition to the FedRAMP Program Management Office, which is housed in TTS;
- Private sector — includes practically every important IT provider ranging from the largest (e.g., Google, Microsoft) to diverse small businesses;
- Agencies — are FedRAMP's key "customers" whom FedRAMP works with to identify and authorize CSOs with cloud services needed by the federal government.

4. FISCAL YEAR 2017/2018 BUDGET IMPACT:

The Federal Citizen Service Fund (FCSF) appropriation for the TTS Office of Products and Programs, and correspondingly the FedRAMP program, remains flat. As the needs of federal agencies to use cloud providers continues to grow and the pipeline of CSOs entering the FedRAMP approval pipeline grows, the FCSF will either need addtional funding to support the robust security and authorization reviews or reduce investements into other programs.

cloud.gov

TTS is building a Platform as a Service called cloud.gov that provides a mix of government compliance with private sector best practices, allowing agencies to securely move their data and services to the cloud. cloud.gov provides government developers an easy to use, secure, scalable platform that meets federal security regulations and saves time and money.

a. Issues:

- Approved Fedramp Authorization: To scale the platform for government-wide use, cloud.gov needs FedRAMP Authorization. This certification will provide a government-wide Authority to Operate (ATO), promoting client-agency

confidence that cloud.gov meets all security requirements. This authorization is currently in process and expected to be granted by Q2 FY17.

- Agency Adoption: In order for cloud.gov to generate government-wide savings and serve as an innovation catalyst, it has to be adopted widely across government. This requires change management and would require agency CIOs and Chief Information Security Officers to change their risk postures and migrate from data ceneters to secure cloud systems.

5. **SCOPE AND EFFECT:**

   a. Impact on GSA's Customers:

      - Creating a shared service that centralizes core security, compliance, and infraustructure requirements will help GSA's customers transition to the cloud more quickly, while saving money and improving security.
      - Developers will have greater agility, be able to iterate more quickly on solutions, and will receive public and stakeholder feedback faster. Entirely new systems can be set up in days rather than months, and new releases can be done in minutes rather than days. GSA's solution has the potential to save massive amounts of time, operating costs, and opportunity costs.
      - By implementing industry best practices, agencies will now be able to provide a standarized environment where government contractors and government developers have a known and familiar solution to work with, rather than having to adapt to each agency's unique solution.

   b. Impact on the Private Sector and State & Local Governments:

      - cloud.gov is working with the private sector to enable more competition in the federal cloud industry. By showing that it is possible to have a cloud environment that is secure, easy to use, and compliant, cloud.gov is enabling vendors to provide government compliant solutions.
      - The cloud.gov platform makes deployment and compliance easier not only for government agencies but also for the vendors looking to work with them. This expands the pool of possible vendors and enables more companies to work with the government.

6. **ACTION(S) PLANNED OR REQUIRED:**

- Recieve FedRAMP JAB Authorization: cloud.gov is on track to receive a FedRAMP JAB Authorization by Q2 FY 2017. This authorization will allow for much broader use of cloud.gov by federal agencies.
- Increase adoption: cloud.gov is working with multiple agencies to move systems to the platform and to enable new systems to be developed or procured within it.
- Provide tools to speed up compliance: the cloud.gov team is building new tools (Compliance Toolkit) to help agencies create all necessary documentation and to help

automate the security processes so each system can receive an ATO faster and with fewer hurdles.

7. **KEY STAKEHOLDER INTEREST:**

- cloud.gov will comply with several statutory and policy requirements set by the White House, GAO, and OMB including, but not limited to:
    - **White House:** Cloud First - *Federal Cloud Computing Strategy, 2011*
    - **GAO:** IT Savings - *Cloud Computing: Additional Opportunities and Savings Need to Be Pursued, 2014*
    - **OMB:** PIV, TIC, etc - Cybersecurity Strategy and Implementation Plan, 2015

8. **FISCAL YEAR 2017/2018 BUDGET IMPACT:**

cloud.gov has received an approved executive business case and associated funding from the GSA Investment Review Board. cloud.gov is required to recover this investment through the fees charged to customers.